

# OFFICIAL FILE COPY

## UNITED STATES MARINE CORPS

1st Marine Division  
(-) (REIN), FMF  
MP PENDLETON, CA 92055

2nd Marine Division  
(-) (REIN), FMF  
CAMP LEJUNE, NC 28542

3rd Marine Division  
(-) (REIN), FMF  
FPO SAN FRANCISCO, CA 96602

JOINT DIVO P3430.4  
3rd MARDIV 7/D37rad  
1st MARDIV 4  
2nd MARDIV 4  
22 May 1984

### JOINT DIVISION ORDER P3430.4

From: Commanding General  
To: Distribution List

Subj: Standing Operating Procedure (SOP) for Electronic Warfare  
(EW) (Short Title: EW SOP)

Ref: (a) JCS Pub. 1  
(b) MCO 3430.3A  
(c) MCO 3430.2A  
(d) FMFM 2-3

Encl: (1 LOCATOR SHEET

1. Purpose. To establish the standing operating procedures for Electronic Warfare within the 1st, 2d, and 3d Marine Divisions, FMF, within the provisions of references (a) through (d).

2. Cancellation. 1st MarDivO P003430.3, 2d MarDivO 3430.1, 3d MarDivO P03430.3.

3. Background. The concept of unit deployment within the Marine Corps makes it necessary to standardize many procedures among the three Marine Divisions. This will enable the deploying units to continue to function effectively regardless of location with the ultimate benefit being that units can come together in the MAGTF environment with enhanced operational effectiveness.

4. Recommendation. This SOP should be reviewed annually and suggested changes submitted to the Commanding General, 3d Marine Division, (SC-7) via the appropriate chain of command. Printed changes to this SOP will be effected through page inserts. When the nature of the change is of sufficient urgency, an advance change will be published by routine directive. Each printed change will incorporate all advance changes promulgated since the previous printed change.

5. Responsibility. The Assistant Chief of Staff, G-3 will be the coordinator for this SOP.

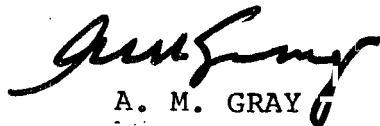
6. Distribution. The Division Adjutant (Central Files) will be the distribution point for this directive.

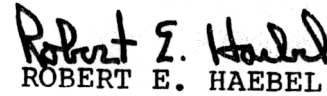
JtDivO P3430.4

22 May 1984

7. Certification. Forwarded and approved this date.

  
E. C. CHEATHAM, JR.

  
A. M. GRAY

  
ROBERT E. HAEBEL

**DISTRIBUTION**

CG, 1st MarDiv List D plus G-3 (3); CG, 2d MarDiv  
List A; CG, 3d MarDiv List A

Copy to: CMC (Code INT), CMC (Code LMW) (1) CG, FMFPac (1) CG,  
FMFLant (1); 1st RADBn (1), 2d RADBn (1).

JtDivO P3430.4  
22 May 1984

LOCATOR SHEET

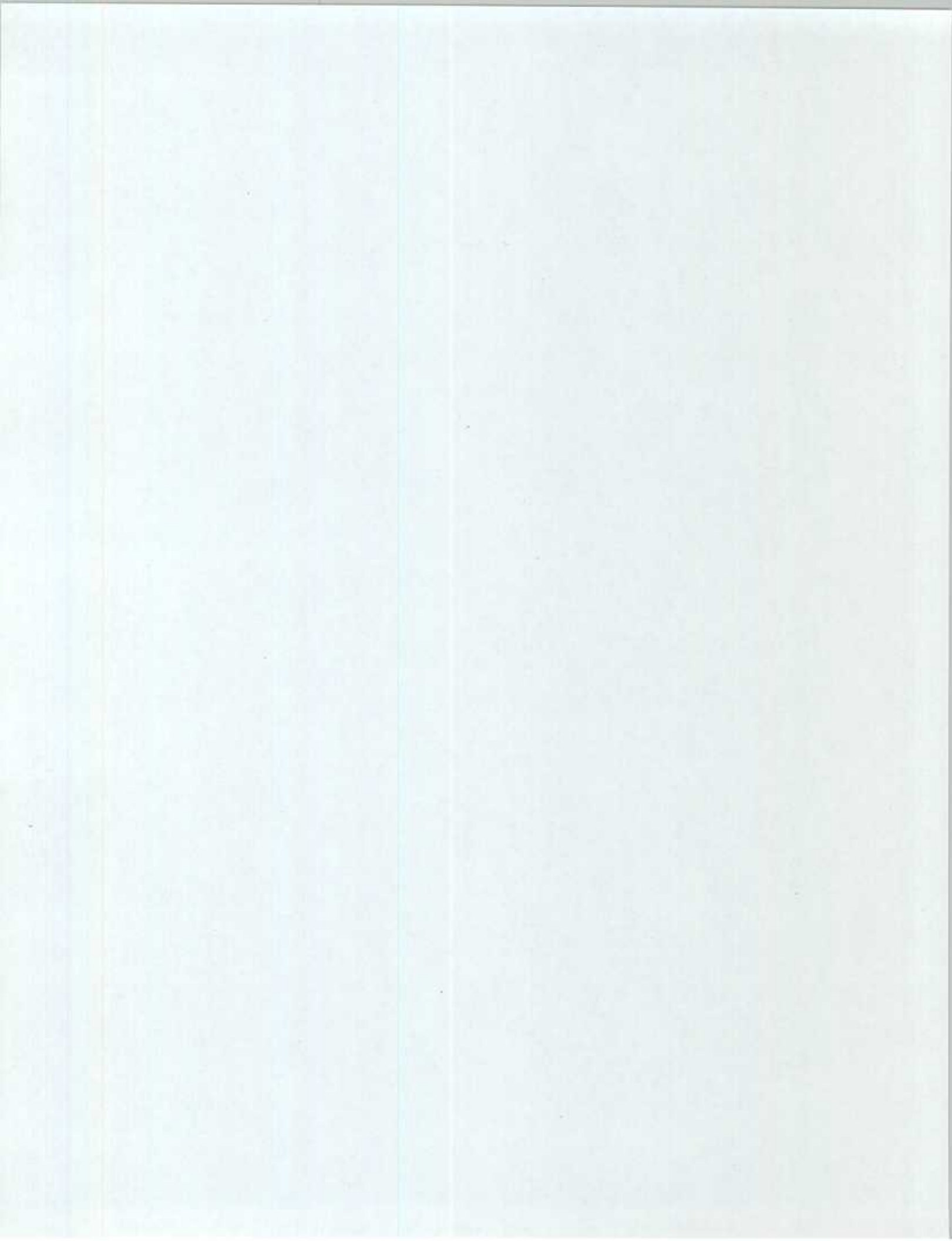
Subj: Standing Operating Procedure (SOP) for Electronic Warfare  
(EW) (Short Title: EW SOP)

Location:

(Indicate the location(s) of the copy(ies) of this  
Manual)

ENCLOSURE (1





# EW SOP

## TABLE OF CONTENTS

### CHAPTER

- 1 INTRODUCTION
- 2 ELECTRONIC WARFARE POLICY
- 3 RESPONSIBILITIES
- 4 REQUIRED REPORTS
- 5 ELECTRONIC COUNTER-COUNTERMEASURES

### APPENDIX

- A GINGERBREAD PROCEDURES
- B BREADWINDOW PROCEDURES
- C MIJI REPORT FORMAT
- D STOP-BUZZER PROCEDURES AND FORMAT
- E FREQUENCY INTERFERENCE REPORT
- F DIRECTIVES AND PUBLICATIONS
- G EW REQUESTING PROCEDURES AND FORMAT



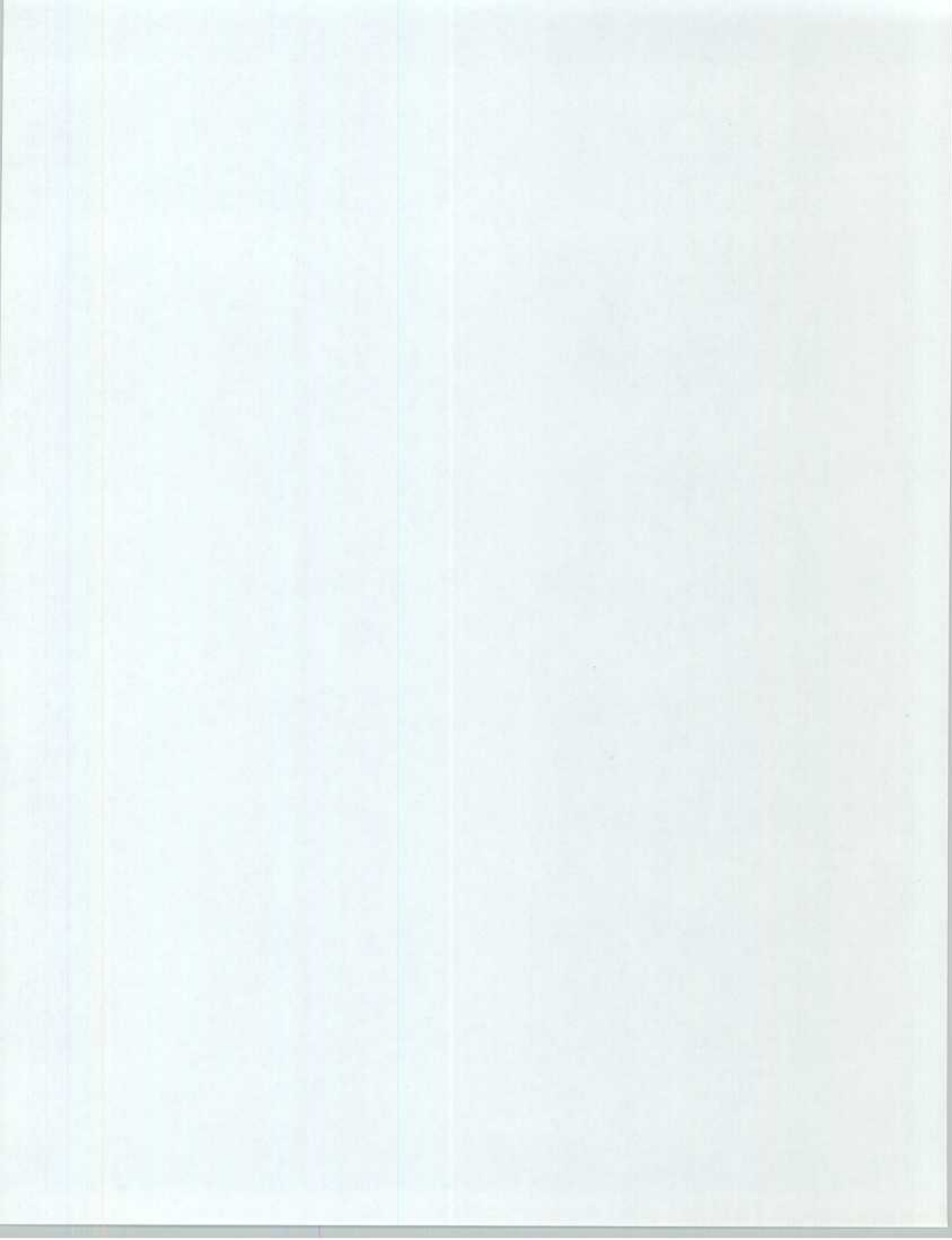
EW SOP

CHAPTER 1

INTRODUCTION

	<u>PARAGRAPH</u>	<u>PAGE</u>
GENERAL.....	1000	1-3
DEFINITIONS.....	1001	1-3
SCOPE.....	1002	1-6





## EW SOP

### CHAPTER 1

#### INTRODUCTION

1000. GENERAL. The modern battlefield will not only display the customary perspective (depth, width, and air space) of previous wars; it will have an added perspective--the fourth dimension of the electromagnetic spectrum. This spectrum is an invisible medium which saturates the battle area and beyond, and upon which the use of our electronic systems depends. Electronic warfare (EW) has evolved to a point where it now constitutes a clearly identifiable element of combat power. The ability of a unit to function as an effective tactical force will greatly depend on its ability to counter an increasingly hostile electromagnetic environment. To fight within this environment the Marine commander will have to depend on EW to prevent the enemy from controlling this vital spectrum. A commander who is unable to quickly and effectively deploy his force because of an inability to communicate with subordinates will find his opportunities for success sharply curtailed. Electronic Warfare cannot take or hold ground, destroy a tank or aircraft or repel an attack. It can, however confuse, deceive, delay, disorganize, and target the enemy when integrated into the concept of operations. When all considerations are equal, victory may go to the force that effectively integrates electronic warfare.

1001. DEFINITIONS. EW is that military action which involves the use of electromagnetic energy to locate, identify, exploit, reduce or prevent hostile use of the electromagnetic spectrum, and to retain friendly use of the electromagnetic spectrum. EW is an essential element of combat power. Its contribution lies in exploiting enemy weaknesses, protecting freedom of action, and reducing security and communication vulnerability.

1. Electronic Warfare Support Measures (ESM). ESM is action taken to search for, intercept, identify, and/or locate sources of radiated electromagnetic energy for the purpose of immediate threat recognition. Thus, ESM provides a source of information required for immediate action involving Electronic Countermeasures (ECM), Electronic Counter--Countermeasures (ECCM), avoidance, targeting, and other tactical employment of forces.

(a) Direction Finding (DF). DF involves the use of highly directional antennas to determine the direction from which a given electromagnetic signal is originating. Normally three or more DF sets are used to make up a network giving more accurate locations.

(b) Line of Bearing (LOB). LOB is the data obtained when a single DF set is used and an azimuth is determined on the signal being targeted.

(c) CUT. CUT is the data obtained when two DF sets are used at locations well separated from one another. Two azimuths are obtained and plotted. The point at which they cross is the CUT. It is a very inaccurate way to locate but it will give a general location.

(d) DF FIX. A DF FIX is the data obtained when three or more DF sets are used. The locations of the units will be as far from each other as possible. When the three (or more) azimuths are plotted, the point at which they intersect will determine the fix which is the most accurate position.

2. Electronic Countermeasures (ECM). The part of EW involving actions taken to prevent or reduce an enemy's effective use of the electromagnetic spectrum. ECM includes:

a. Electronic Jamming. The deliberate radiation, reradiation, or reflection of electromagnetic energy with the objective of disrupting the use of electronic devices, equipment, radar, or systems being used by an enemy.

(1) Spot Jamming. When the power of the jamming unit is concentrated on one particular frequency within the spectrum.

(2) Barrage Jamming. When the power of the jamming unit is spread over a wide portion of the frequency spectrum jamming three or more frequencies at the same time.

(3) Sweep Jamming. When the jamming signal moves through the spectrum continuously jamming pre-set frequencies one at a time for a fraction of a second then continuing to the next frequency.

b. Electronic Deception. The deliberate radiation, reradiation, reflection, alteration, absorption, or enhancement of electromagnetic energy to mislead the enemy in the interpretation of what is received from his systems. Electronic deception falls into two categories:

(1) Manipulative Communications Deception (MCD). MCD is the radio communications aspect of the alteration or simulation of friendly electromagnetic radiations to accomplish deception.

(2) Imitative Communications Deception (ICD). The introduction of radiations into enemy channels which imitate their own emissions to introduce error or confusion into the enemy's command and control procedures through deception of their electronic equipment operators.

3. Electronic Counter-Countermeasures (ECCM). The part of EW involving actions taken to ensure friendly use of the electromagnetic spectrum against enemy EW. Further definitions under this section of EW are as follows:

a. Authentication. A security system designed to protect a communications system against acceptance of a fraudulent transmission, message or originator. Radio operators at all levels shall be familiar with these procedures.

b. Brevity Codes. A code which provides no security but which has as its sole purpose shortening the transmission time of messages rather than the concealment of their content. A combination of, normally two, number/letter configurations that have a predetermined meaning used to reduce transmission time of a message, not to be used for encryption. The Brevity List is an unclassified publication.

c. Evasion Methods. Methods employed to deny hostile forces the opportunity to collect or locate electromagnetic emissions radiating from friendly communications or radar systems.

d. Covered Net. A radio net which, with the addition of encryption equipment, may be used to pass classified or sensitive information. Internal content of the traffic cannot be derived by intercept.

e. Land Line. The use of wire in point to point communications which minimize the enemy collection opportunities due to the lack of electromagnetic radiations.

f. Terrain Masking. Using natural terrain features between friendly electronic emitters and hostile units for the purpose of reducing or denying the enemy the opportunity to collect communications of friendly force.

g. GINGERBREAD. A term used by U.S. forces when it is recognized that a hostile or enemy communicator is attempting to or has entered into a friendly communications net for the purpose of Imitative Deception. See Appendix A.

h. BEADWINDOW. A term used when a violation/compromise has, or is about to, happen during the course of communications between two stations on given net. This violation/compromise would be one of the Essential Elements of Friendly Information (EEFI's). See Appendix (B).

i. Meaconing, Intrusion, Jamming, Interference, (MIJI) Reporting. A process of information exchange concerning the active employment by the enemy of one or several EW tactics against friendly units or aircraft. This process alerts the commander to significant enemy action. See Appendix (C) for format. The current edition of MCO 3430.3 states Marine Corps policy on the MIJI Report program.

j. Emission Control (EMCON). The selective control of emitted electromagnetic or acoustic energy to minimize its detection by enemy sensors or to improve the performance of installed friendly sensors.

k. Communication Security (COMSEC). COMSEC results when all measures designed to deny unauthorized persons information of value which might be derived from the possession and study of telecommunications are utilized. Measures designed to mislead unauthorized persons in their interpretation of the results of such possession and study must also be used.

l. Transmission Security (TRANSEC). TRANSEC is the component of COMSEC which results when all measures designed to protect transmissions from interception and exploitation by means other than cryptanalysis are utilized.

m. STOP-BUZZER. A term used in radio communications anytime a dangerous situation occurs. This term, when passed by the fastest means available, will stop ECM operations on the spot until the all clear is given by the Division G-3. See Appendix (D).

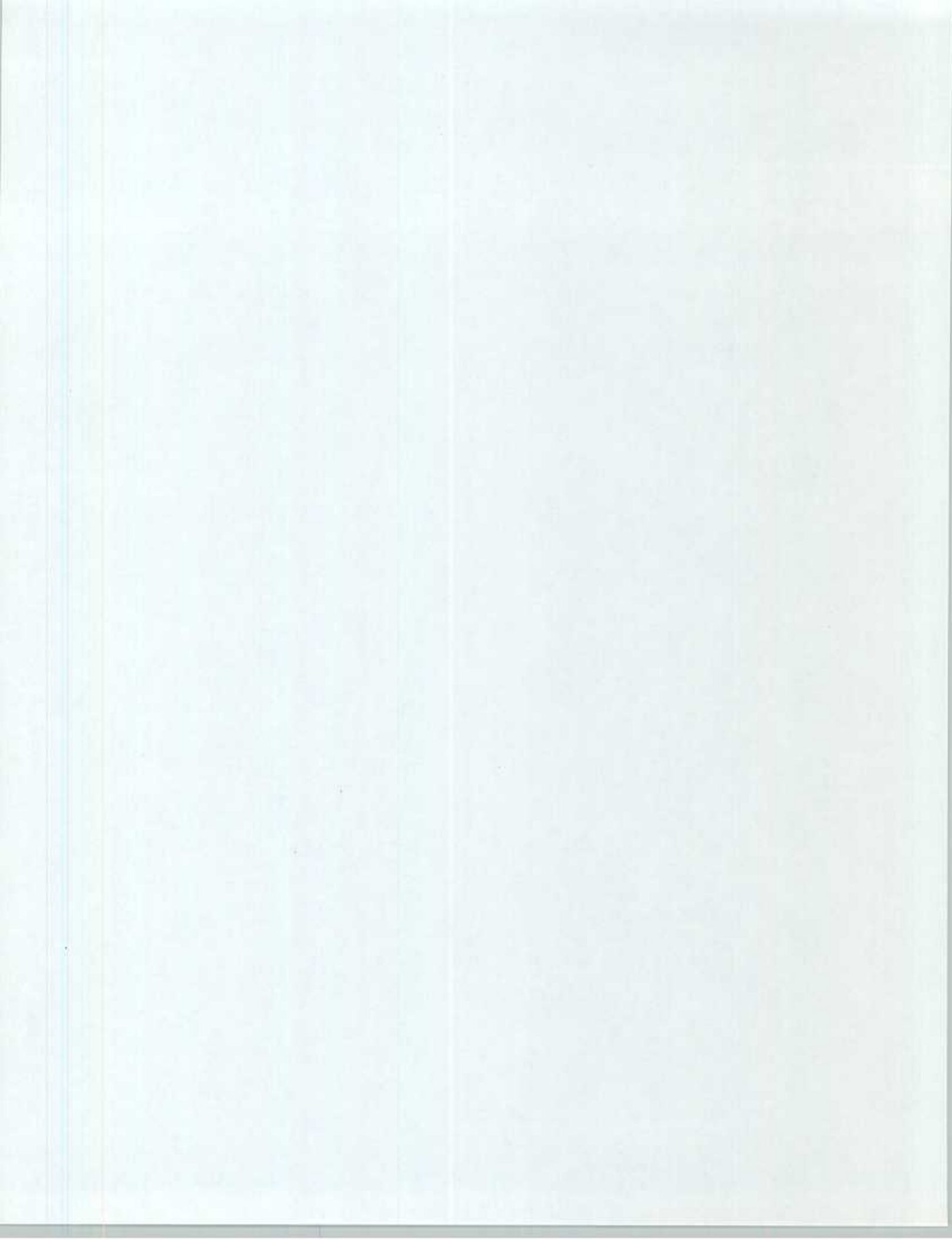
1002. SCOPE. During any battle, a modern military force depends on electronics for communication to maintain command and control of forces and the employment of radar and weapon systems. Because of this dependence on electronic systems and devices, Marine forces, as well as enemy forces, are vulnerable to actions which can reduce the effectiveness of these devices or gain intelligence from them. An EW system that enables the commander to degrade the effectiveness of enemy electronic activities is a powerful weapon that can be used to support both offensive and defensive operations. EW can confuse, deceive, delay, disorganize and locate enemy targets when integrated into the concept of operation and used intelligently by a commander as an asset and integral part of his combat planning.

EW SOP

CHAPTER 2

ELECTRONIC WARFARE POLICY

	<u>PARAGRAPH</u>	<u>PAGE</u>
GENERAL.....	2000	
OBJECTIVES.....	2001	
POLICY.....	2002	



## EW SOP

### CHAPTER 2

#### ELECTRONIC WARFARE POLICY

2000. GENERAL. EW is a command responsibility. The Commanding General has directed the establishment of a progressive EW training program within each major operational unit. To this end, every commander and staff officer must have knowledge of how EW can be effectively employed. This includes the capabilities and limitations of EW units, such as Radio Battalions and the Tactical Electronic Warfare Squadron (VMAQ-2), and their respective support equipment. The EW policy set forth in this section implements this program, and is applicable to all Division units. The current edition of MCO 3430.2 provides Marine Corps policy for the conduct of EW.

#### 2001. OBJECTIVES

1. To provide all Marines with an understanding of EW as an element of combat power which must be thoroughly integrated and coordinated in offensive and defensive operations.
2. To instill in commanders an appreciation for the necessity that exercise scenarios be conducted in a dense EW environment, thus ensuring that their Marines develop the expertise to counter potential enemy initiatives.
3. To instill in commanders an appreciation for the need to establish EW education as a high priority in their operational efforts.

#### 2002. POLICY

1. Within the division, the responsibility for the planning and implementation of EW rests with the G/S-3; however, the overlapping nature of EW demands that close and continuous coordination be maintained within the staff elements, and in particular with the G/S-2 (Intel and SIGINT Plans Officers) and the CEO/Unit Communication Officer. Only through the merging of information/coordination from all concerned staff planning agencies, can the commander be realistically advised of the advantages of employing available EW resources.
2. A unit's ability to successfully contend with an intense EW environment is based primarily on three factors:
  - (a) Command interest, as demonstrated in the conduct and maintenance of appropriate EW training programs.
  - (b) Inclusion of EW within the unit's operational orders as an appendix thereto.



(c) Unit perceptions and subsequent employment of basic ECCM principles.

3. All commands will maintain a vigorous ECCM program that will include at the minimum:

(a) Maximum training of electronic equipment operators and associated personnel in ECCM techniques and procedures.

(b) Indoctrination and training of command, staff, and operation personnel in the capabilities and limitations of electronic equipment when operated in a hostile EW environment.

(c) Signal security (SIGSEC) training.

4. In support of each command's ECCM program, commanders will ensure that their units maintain the capability to operate under stringent Emission Control (EMCON) conditions on short notice and for extended periods of time.

5. Incidents of electromagnetic interference during exercises and real time situations will be reported immediately by use of the Frequency Interference Report (FIR) simultaneously to CEO/SYSCON G/S-3, G/S-2, and if available, supporting EW elements.

6. Appendixes may be published by each division on specifics of their EW program. Commanders are encouraged to expand on the basic guidance whenever possible.

EW SOP

CHAPTER 3

RESPONSIBILITIES

	<u>PARAGRAPH</u>
GENERAL.....	3000
COMMANDERS'S RESPONSIBILITIES.....	3001
ASSISTANT CHIEF OF STAFF, G-2.....	3002
ASSISTANT CHIEF OF STAFF, G-3.....	3003
COMMUNICATION-ELECTRONICS OFFICER.....	3004
ELECTRONIC WARFARE OFFICER.....	3005

CHAPTER 3  
RESPONSIBILITIES

<u>PAGE</u>	<u>PARAGRAPH</u>
3000	GENERAL.....
3001	COMMANDERS'S RESPONSIBILITY
3002	ASSISTANT CHIEF OF STAFF G-2
3003	ASSISTANT CHIEF OF STAFF G-3
3004	COMMUNICATION-ELECTRONICS OFFICER
300	ELECTRONIC WARFARE OFFICER.

## EW SOP

### CHAPTER 3

#### RESPONSIBILITIES

3000. GENERAL. Responsibility for EW is not restricted to the commander or to a particular group of individuals. It is a continuing responsibility of all individuals who prepare, plan, or conduct operations and training, or have cognizance and/or control of electronics systems. General responsibilities for EW are contained in the following paragraphs. Specific responsibilities are contained in Chapter 1 of MCO 3430.2.

3001. COMMANDER'S RESPONSIBILITIES. Because EW, SIGINT, and SIGSEC are vital elements in the readiness of all Marine units, commanders must ensure that their units and staffs are aware of the threat, are knowledgeable of methods and techniques, and are prepared to conduct operations in any SIGINT/EW environment. This readiness includes both the organic and specialized units under their cognizance. Unit commanders shall:

1. Designate an officer from the S-3 section as the Electronic Warfare Officer. A copy of the appointing letter/order will be forwarded to Division Headquarters (ATTN: G-3/EWO).
2. Ensure accomplishment of EW training in accordance with this SOP.
3. Request staff assistance visits by the Division EWO, as necessary, in order to expand and present unit EW training or assist unit EWO.

#### 3002. ASSISTANT CHIEF OF STAFF, G-2

1. Provides EW threat information and monitor and coordinate the intelligence information aspects inherent in EW operations.

2. Participates and coordinates with the G-3 in the preparation of EW plans and appendices.

#### 3003. ASSISTANT CHIEF OF STAFF, G-3

1. Maintains primary staff responsibility for the planning, conduct, and supervision of the Division EW program.
2. Assigns the Division EW Officer (EWO) from the Operations Section.

3004. COMMUNICATION-ELECTRONICS OFFICER. Coordinates all matters pertaining to the electromagnetic environment in the command to

include frequency allocation, assignment, use, and review to reduce all source electromagnetic interference.

3005. ELECTRONIC WARFARE OFFICER

1. Division Electronic Warfare Officer (EWO). The Division EWO shall:

a. Assist the Division Communication-Electronics Officer (CEO), as required, in arranging ECM/ECCM training in accordance with current directives.

b. Submit required reports in accordance with this SOP.

c. Provide assistance and direction, as may be required by division units relative to planning, coordination, and execution of EW matters.

d. Manage/coordinate EW formal schools with G-3 Training and higher headquarters as required.

e. Prepare and maintain current files on EW plans, policies and doctrine; coordinate all EW related activities within the division; maintain working liaison with EWOs of higher and lower echelons; initiate and maintain a vigorous EW awareness program; and advise the Division Staff on all matters pertaining to EW operations.

f. Ensure coordination/liaison with other Division Staff elements and radio battalion operations section in order to accomplish the established EW training.

2. Unit Electronic Warfare Officer. The unit EWO shall:

a. Be thoroughly familiar with the contents of this SOP and other EW related publications.

b. Initiate and maintain vigorous EW awareness training programs in a coordinated effort with the Division EWO.

c. Supervise EW training for the unit and coordinate all levels of training with appropriate Division Staff elements.

d. Submit the reports required herein.

e. Coordinate EW matters with the Division EWO, CEO, G-2 as required.

f. Be thoroughly familiar with EW operations, planning and tasking, EW relationship, hostile EW capabilities, and current EW documentation.

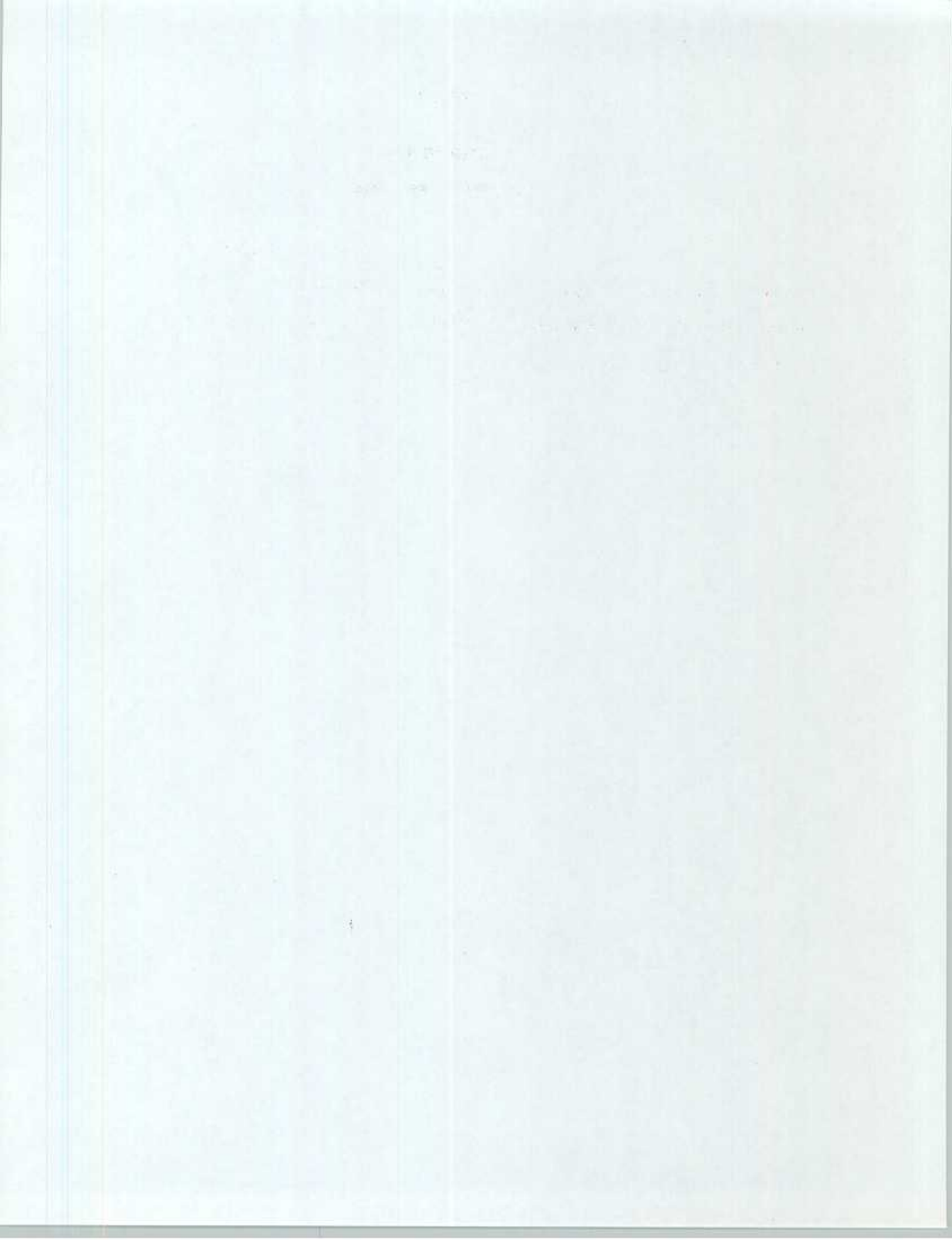
g. Successfully complete Marine Corps Institute (MCI) 25.26 Introduction to EW and MCI 25.25 Communications Security.

EW SOP

CHAPTER 4

REQUIRED REPORTS

	<u>PARAGRAPH</u>	<u>PAGE</u>
GENERAL.....	4000	4-3
FREQUENCY INTERFERENCE REPORT (FIR).....	4001	4-3
MIJI REPORT.....	4002	4-3
STOP-BUZZER REPORT.....	4003	4-3



## EW SOP

### CHAPTER 4

#### REQUIRED REPORTS

4000. GENERAL. Electromagnetic emissions by their nature are vulnerable to natural and man-made interferences. Both require corrective action, usually within relatively short time frames. The following paragraphs describe the interference reporting programs.

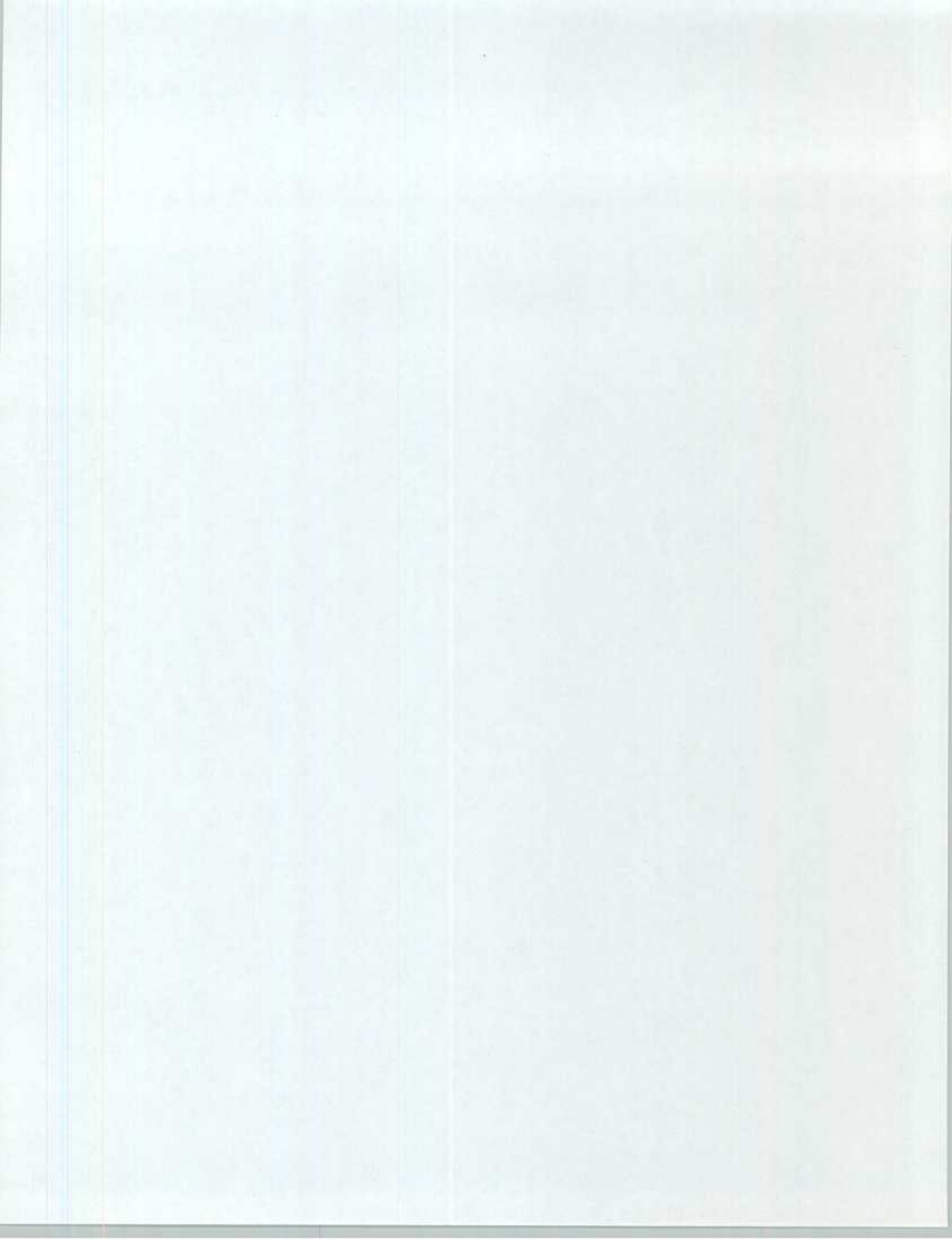
4001. FREQUENCY INTERFERENCE REPORT (FIR). The FIR is the communicator's vehicle for immediately reporting interference being experienced. The FIR is passed as quickly as possible, via whatever means are available, in order to alert friendly EW and CEO personnel.

1. The FIR provides rapid alerting of friendly EW personnel to allow them the opportunity to take corrective action as necessary.
2. Simultaneously, the FIR provides the communication planners an immediate report that may relate to communication system problems. That is, interference experienced by the individual communicator may be corrected through procedures directed by the communication planners rather than through EW resources, i.e., frequency reallocation, equipment redistribution, etc.
3. The FIR, when formatted as directed, is unclassified, and can be passed over any communication circuit or other communication method, i.e., telephone, runner, etc.
4. The FIR format is simple and easy to read. See Appendix E.
5. Time is critical. Report interference as soon as possible. The report should be submitted before the interference ends if possible.

4002. MIJI REPORT. The MIJI report is the second step in reporting interference. The MIJI Report is a detailed report of the interference incident, and as such will not be as timely as the FIR. The MIJI Report will not be initiated unless requested by higher echelon or local G/S-2. Once requested, the format provided in the current edition of MCO 3430.2 will be utilized. Local format MIJI Reports may be requested to fulfill particular operational (exercise) or training needs. See Appendix C.

4003. STOP-BUZZER REPORT. This report is required any time the operator or any other individual feels there is a dangerous or emergency situation about to/has occurred. This report (with no set format) will be sent by the fastest means to the EW element involved in the exercise/operation, so that the friendly ECM efforts causing the emergency situation will be terminated. See Appendix D. The Stop-Buzzer net shall be monitored by all units conducting ECM. This net is established by the command (net control) whose units are subject to ECM. In joint/combined exercises and operations, the joint/combined commander publishes Stop-Buzzer procedures.



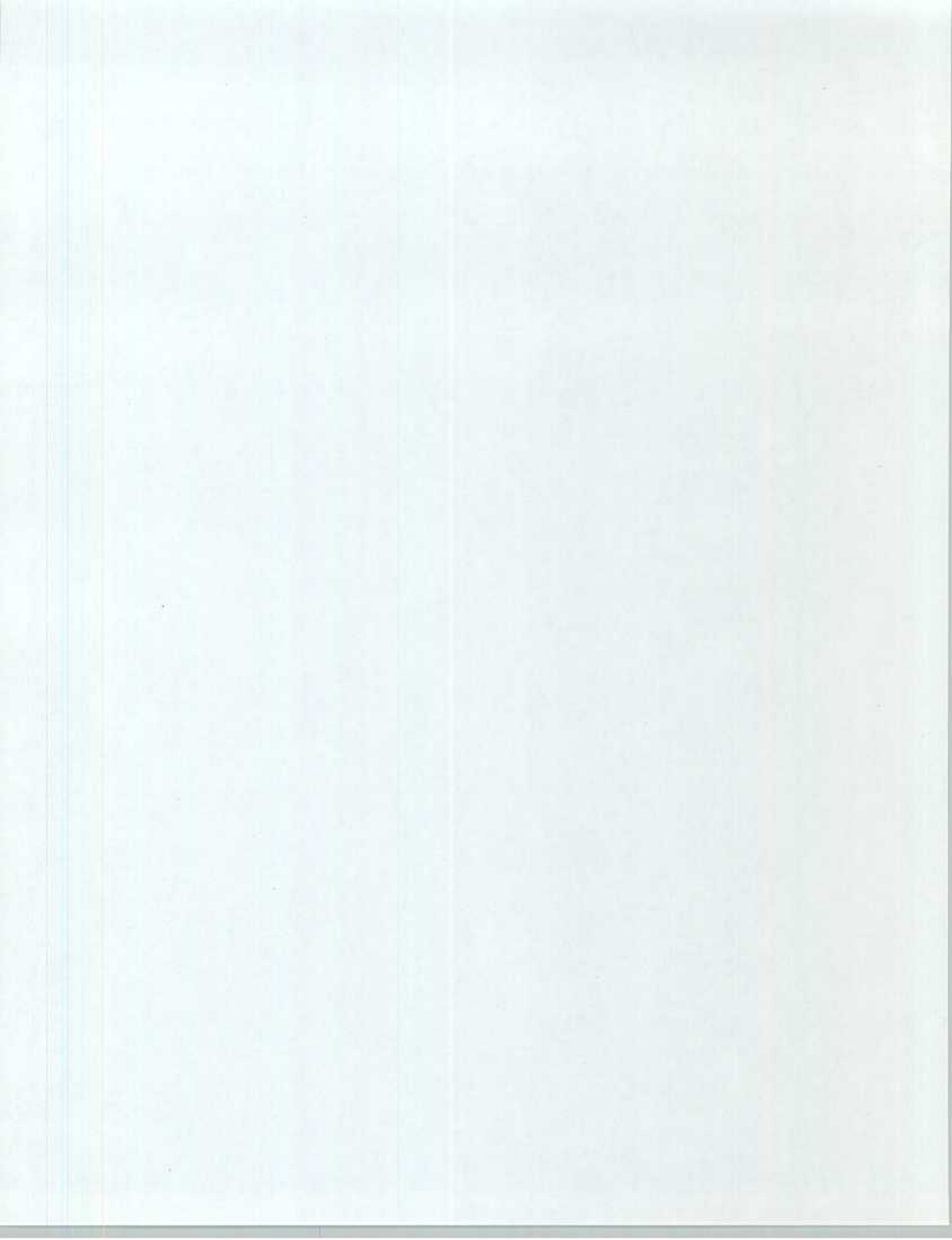


EW SOP

CHAPTER 5

ELECTRONIC COUNTER-COUNTERMEASURES

	<u>PARAGRAPH</u>	<u>PAGE</u>
GENERAL.....	5000	5-3
PREVENTIVE ECCM.....	5001	5-3
REMEDIAL ECCM.....	5002	5-4
DEFEAT OF ADVERSARY RADIO DIRECTION FINDING.....	5003	5-6



## EW SOP

### CHAPTER 5

#### ELECTRONIC COUNTER-COUNTERMEASURES

5000. GENERAL. EW operations, like the electromagnetic spectrum they attack, will vary in power and orientation. As such, they can be degraded or defeated. The following paragraphs provide preventive/remedial actions that can be successful in maintaining a command's electronic counter-countermeasures (ECCM) posture.

5001. PREVENTIVE ECCM. Those measures taken to prevent or avoid adversary EW. The primary objective of preventive ECCM is to defeat electronic warfare support measures (ESM); that is, to keep the adversary from monitoring and targeting friendly communication frequencies.

1. Emission Control (EMCON). The system employed to make maximum use of radio silence, alternative non-radio means of communication, and other means to prevent the enemy from intercepting friendly communications.

2. EMCON Plan. A well prepared EMCON plan should be an essential part of the ECCM annex/communication plan. It should outline, step-by-step the procedures and techniques the unit employs to ensure effective EMCON. These techniques would normally include:

a. Proper radio discipline - The use of proper radio procedure reduces the transmission time required to send messages and makes messages more comprehensible with fewer readbacks.

b. Strict radio discipline - This involves strict net control. Net control should communicate with stations individually or collectively. Each station should wait its turn to communicate, rather than compete to get traffic through. Long and difficult words in texts should be avoided and simpler more concise words should be used. Radio checks should be kept to a bare minimum.

c. Brevity codes - Brevity codes represent a much more rapid means of sending traffic; however, they must be understood by all if they are to be employed. Brevity codes shall not be classified, as they do not provide security for transmissions; they simply shorten transmission times. Brevity codes are also recommended for use on secure circuits to reduce transmission times.

d. Directional antennas - The use of directional antennas greatly reduces the possibility of intercept. They should be employed so that major transmission lobes extend only into friendly territory. Directional antennas are also more difficult to jam.

e. Antenna masking - Antenna masking is an important technique in preventing an adversary from intercepting friendly signals. The object is to place terrain features or other significant obstacles

between friendly and adversary antennas. The use of hills, valleys, canyons, buildings, walls, etc., can serve this purpose.

g. Low power - The low power setting on communications equipment, where applicable, should always be used. Using high power extends the distance of communications equipment, thereby making it more vulnerable to intercept.

h. Squelch discipline - Some jamming systems have a squelch capture effect that prevents a radio from receiving any signal when the squelch is in the on position. If squelch must be used, periodic on-off checks will ensure viable communications continue.

i. Wire/landline - Wire is one of the best alternative means of communications in a hostile EW environment. It is limited by availability and difficulty of installation. Rapid wire laying techniques must be exercised and used.

j. Arm and hand signals - Another important alternative means of communicating information is through arm and hand signals. Lower echelon units should not use radio communications when visual conditions allow the use of arm and hand or other visual signals.

k. Flags/pyrotechnics - Flags are another form of visual signal available for short range or ground to air communication, and must be planned for. Pyrotechnics are visible to everyone, and offer another alternative means.

l. Manual morse - Manual morse is an excellent means of communication, and must be taught and planned for. Morse can be used over radio or as a visual signal when radio use is limited. Manual morse signals can break through many jamming signals.

3. Other measures - Other measures include the proper use of the Communication-Electronics Operating Instruction (CEOI), and the use of encryption equipment.

5002. REMEDIAL ECCM - Those measures taken once hostile EW is identified or suspected, to remedy the situation and reestablish effective communications.

1. Defeating jamming. Immediate measures - When a radio operator believes he is being jammed, his first action must be to check his equipment for internal malfunction. This is accomplished by disconnecting his antenna. If the signal disappears, or decreases, the disturbance is external to the equipment. If it does not decrease, it is probably an internal equipment problem.

a. Continue to operate - Although an annoying signal is being experienced, the radio operator must continue to operate as long as possible. He must not acknowledge, over his radio, the presence of the disturbing signal...for to do so will indicate to an adversary that his jamming is effective. If interference becomes such that

## EW SOP

communications cannot be maintained, alternative means must be used. A jammer is highly susceptible to radio direction finding if he stays on the air. The longer the transmission, the longer he will usually maintain his jamming. Also, periodically, a jammer must stop his jamming to "lock through" to see if there are still friendly transmissions. Once again, if transmissions continue, he may conclude that his operations have failed, and discontinue his actions.

b. Switch to high power - If an interrupted signal cannot be overridden in low power, then high power (if available) must be attempted. Grounding a tactical radio will increase its power-out 10% to 15%. Jamming is a precise science, based upon the radiated power of the transmitter to be jammed, the distance between the transmitter and receiver, and the distance of the jammer to the receiver. Increasing power can degrade the precise calculations used to locate that particular jammer.

c. Rapid "burst" transmission - When the operator keys a handset, an adversary will usually key his jammer. As mentioned above, jamming is not usually continuous. When jamming stops, a short two or three word transmission can usually be sent prior to the keying of the jammer once again. Using this technique, whole messages can be transmitted successfully in jamming environment. Messages must be kept short and concise. Good preplanning and prearranged signals facilitate this technique. The jammer affects the receiving end of the transmission, therefore it falls upon the transmitting station, once jamming has been realized, to use this short burst technique to successfully communicate.

d. Parallel circuit - The use of parallel circuits, that terminate in the same area as the receiving station, will provide a successful means of message transmission (if available).

e. Messenger - The use of messengers is an effective means of transmitting communications traffic, and must be planned for and used.

f. Wire and visual - Wire and visual means also provide excellent alternative means of communication.

g. Antenna orientation - Check antenna orientation. As mentioned above, jamming is a precise science. Slight movement of a directional antenna can usually negate hostile jamming operations, and continue to the communication link. Also, when jamming occurs put antenna mast to full height.

h. Antenna polarization - The effects of hostile EW may be reduced by changing antenna polarization. In this case, both transmitting and receiving antenna polarization should remain the same to maintain reliable communications.

i. Frequency switching - Only as a last resort. Units do not have a wealth of available frequencies to use. Changing frequencies tells the adversary jamming he was successful, and he sends his

## EW SOP

signal monitoring assets back to work to find the next frequency. He now knows that his present location and power output are sufficient to degrade the communications a second or even third time. Also, changing frequencies may cause confusion on the net, if all stations are not notified before the change. Prearranged codes or signals can assist in this technique, if used.

2. Defeating Imitative Communications Deception (ICD) - ICD, simply stated is the entering into friendly communications by hostile EW personnel. ICD can be defeated.

a. Authentication - The most effective means of defeating ICD is to perform cautious and proper authentication. Do not over authenticate because the enemy may be preparing a list of the authentications used.

b. ICD will occur when there is poor circuit discipline; peculiarities in operating procedures; large number of stations on net; fast moving situations where message volume is heavy; and lack of proper authentication. Remove the vulnerability, or correct it as found.

c. GINGERBREAD - GINGERBREAD is the codeword indicating an apparent unauthorized or bogus station has intruded into a net. Use this code to alert other stations when an intruder is suspected. Never neglect to "sound the alarm" unless directed not to do so. By keeping quiet, other stations on the net may accept the bogus station as valid, and fall prey to its deceptions.

3. Frequency Interference Report (FIR) - If friendly EW assets and communications planners are not alerted as rapidly as possible on all interference problems, appropriate actions cannot be taken. Report it fast!

5003. DEFEAT OF ADVERSARY RADIO DIRECTION FINDING. Radio direction finding (DF) must rely upon a number of situations to accurately locate a transmitting antenna. The situations are both man-made and natural. The man-made situations can be corrected through the proper techniques.

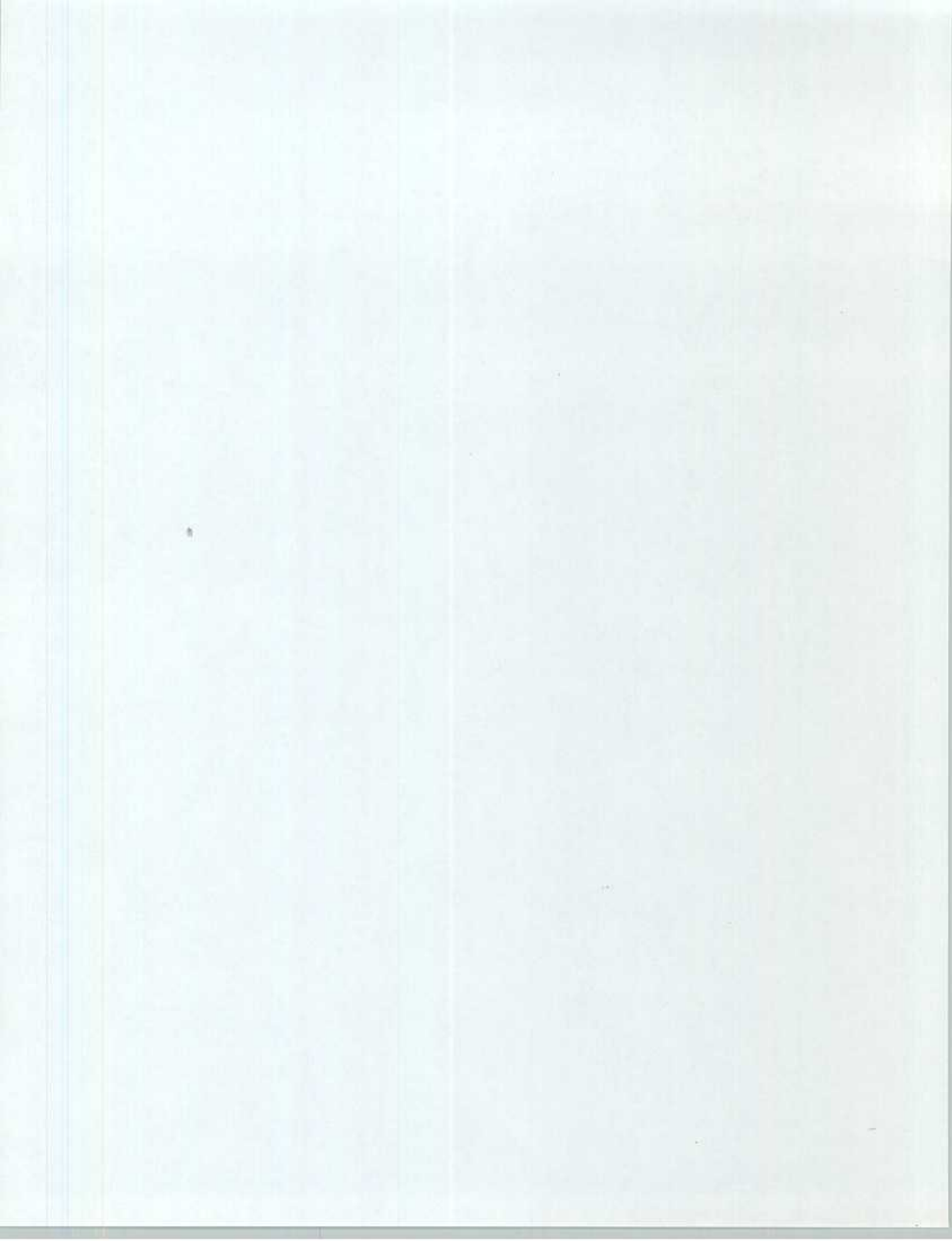
1. Reduce transmission power to minimum levels required to permit effective communication. Do not send traffic beyond the obvious recipient. The greater power-out, the greater the susceptibility to hostile DF operations.

2. Use mobile antennas where practical, and move as much as possible. Degrade adversary DF simply by not remaining at the same locations for long periods of time.

3. Use horizontally polarized directional antennas where the tactical situation permits.

4. Omnidirectional antennas (man-pack whips/tapes) can be made into "tactical directional" antennas. Point the antenna null towards the adversary, thereby creating a side-to-side directional transmission lobe configuration.
5. Remove antennas at least one kilometer, when possible. If adversary DF targets the antenna, at least be away from it. An antenna can be remoted up to two miles under optimum conditions.
6. Use decoy antennas. Adversary intelligence sources use visual sighting as well as DF to locate your antenna.
7. Transmit as quickly as possible, then get off the air. Organize message content beforehand to minimize transmission time. Avoid sending messages by radio if alternative means are available and appropriate timeliness of transmission can be achieved.
8. Plan for and practice alternative communication means.
9. Mask antennas. Site antennas with obstacles between them and the adversary to reduce the possibility of intercept and DF.
10. Use proper authentication procedures. ICD operations are also used to keep operators on the air long enough to DF.
11. Insure that communication personnel are properly trained.
12. Be cautious with the use of radars. They are also vulnerable to DF.
3. Use dummy load (antenna) for maintenance and tuning procedures.
14. Employ random transmissions, rather than working on a schedule, to reduce the adversary's ease of interception and DF.
15. Do not routinely "radio check." More frequent transmissions increase vulnerability to adversary EW operations of all types.
16. Do not peak traffic before an operation or maneuver. Once done, the station will be targeted for extensive adversary EW operations.
17. Target adversary EW assets for ECM or physical destruction. Learn how to react to hostile EW and use the system and reports established to alert friendly EW resources to hostile activity.





EW SOP

APPENDIX A

GINGERBREAD PROCEDURES

1. GINGERBREAD Procedures. The term GINGERBREAD, as described in Allied Communications Publication (ACP) 165, is used to alert net stations that "Voice imitative deception or intrusion is suspected on this net." GINGERBREAD procedures for unsecure voice circuits are as follows:

a. Any station failing to authenticate correctly two times in succession shall be treated as an unauthorized subscriber on the net.

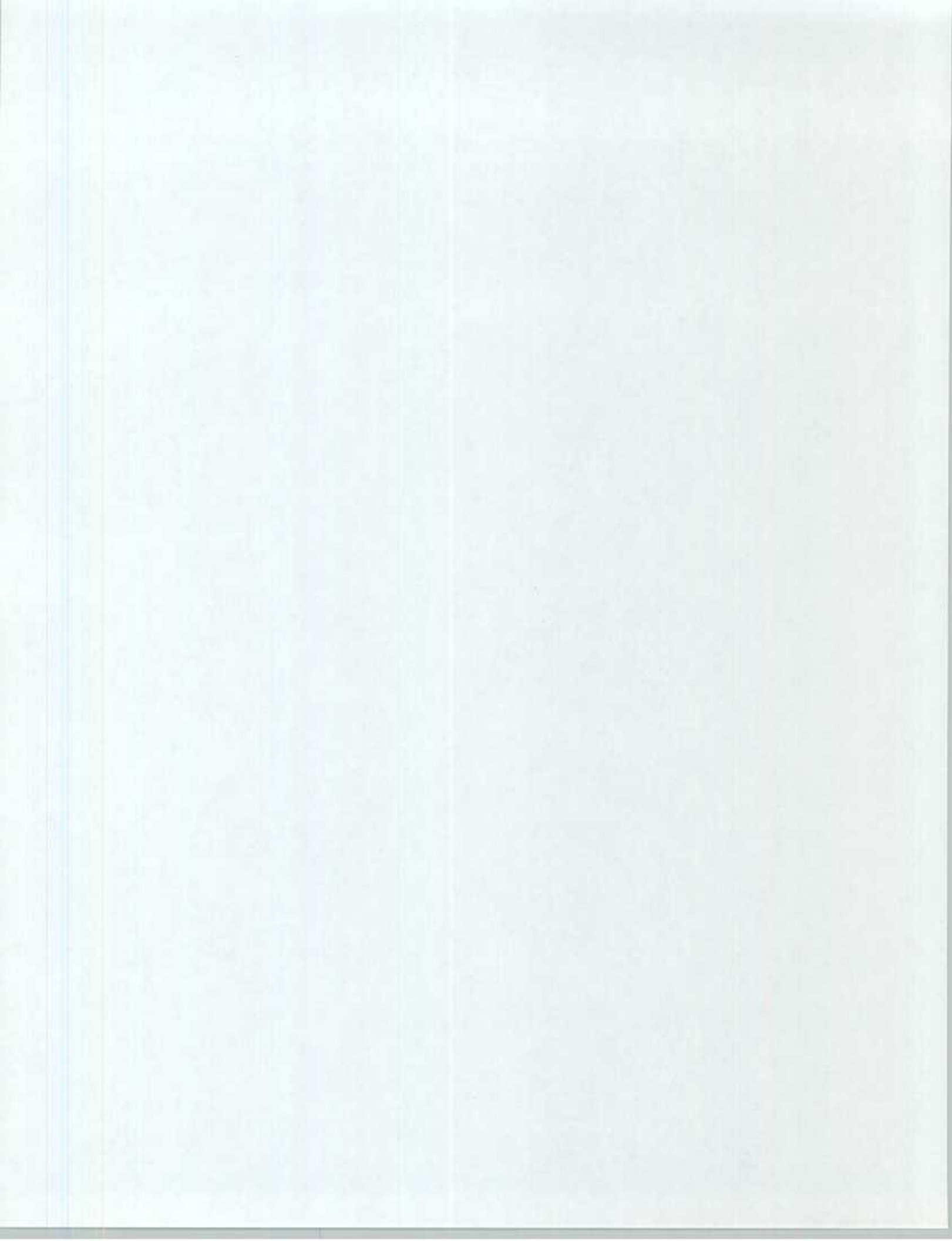
b. Any net operator who suspects there is an unauthorized subscriber on the net will announce the term GINGERBREAD.

c. The station reporting GINGERBREAD will establish its own authentication which may be used to establish further proof of the reporting station's authenticity.

d. The station being imitated should use transmission authentication to validate its transmission.

e. Unauthorized transmissions from the station being imitated will be challenged until the imitating station has apparently abandoned its efforts.

f. The NECOS will submit a MIJI report as soon as GINGERBREAD is announced.



## EW SOP

### APPENDIX B

#### BEADWINDOW PROCEDURES

Some seemingly insignificant slips of communications procedures can result in major compromises of tactical military information that could prove devastating to friendly forces. The compromise of this information can enable the enemy to alter his operations. Therefore, measures should be taken to protect out communications from compromise. One of these communications security precautions is known as BEADWINDOW Procedures.

BEADWINDOW utilizes the following list of Essential Elements of Friendly Information (EEFI's). When an operator makes a transmission revealing an EEFI, any other operator on the net can come up on the net and transmit "BEADWINDOW NUMBER \_\_\_\_ (derived from the EEFI list)". This short message informs not only the operator who made the disclosure, but also other operators on the net, that a possible compromise of an EEFI has occurred. The appropriate response is..."Roger, out".

#### NATO/NAVY/USMC ESSENTIAL ELEMENTS OF FRIENDLY INFORMATION (EEFI)

- |                |   |
|----------------|---|
| 01             | Friendly or enemy position, movement or intended  |
| + Position     | movement: position, course, speed, altitude or destination of any air, sea or ground element unit or force.   |
| 02             | Friendly or enemy operations, intentions,   |
| + Capabilities | composition or identity, capabilities, limitations or significant casualties to special equipment, weapon systems, sensors, units or personnel. Percentage of fuel or ammunition remaining. |
| 03             | Friendly or enemy operations, intentions, progress  |
| + Operations   | or results: operational or logistic intentions; assault objectives; mission participants; flying programs, mission situation reports; results of friendly or enemy operations.              |
| 04             | Friendly or enemy ECM/EMCON intentions, progress or   |
| + EW           | results: intentions to employ ECM, results of friendly or enemy ECM objectives of ECM, results of ESM, present or intended EMCON policy.  |
| 05             | Friendly or enemy key personnel: movement or  |
| + Personne     | identity of friendly or enemy FLAG Officers; distinguished visitors; unit commanders; movements of key maintenance personnel indicating equipment limitations.                              |
| + 06           | Friendly or enemy COMSEC locations: linkage of  |
| + COMSEC       | codes or codewords in plain language; compromise  |

EW SOP

of changing frequencies or linkage with line numbers or circuit designators; linkage of changing call signs with previous call signs of units; compromise of encrypted/classified call signs; incorrect authentication procedures.

- + 07 Wrong Circuit Inappropriate transmission: information requested, transmitted or about to be transmitted which should not be passed on the subject circuit because it either requires greater security protection or it is not appropriate to the purpose for which the circuit is provided.
- 08-10 For NATO assignments as required.
- 11-29 Reserved for CINCUSNAVEUR
- 30-49 Reserved for CINCLANFLT
- 50-69 Reserved for CINCPACFLT

EW SOP

APPENDIX C

MIJI REPORT FORMAT

From: Reporting HQ

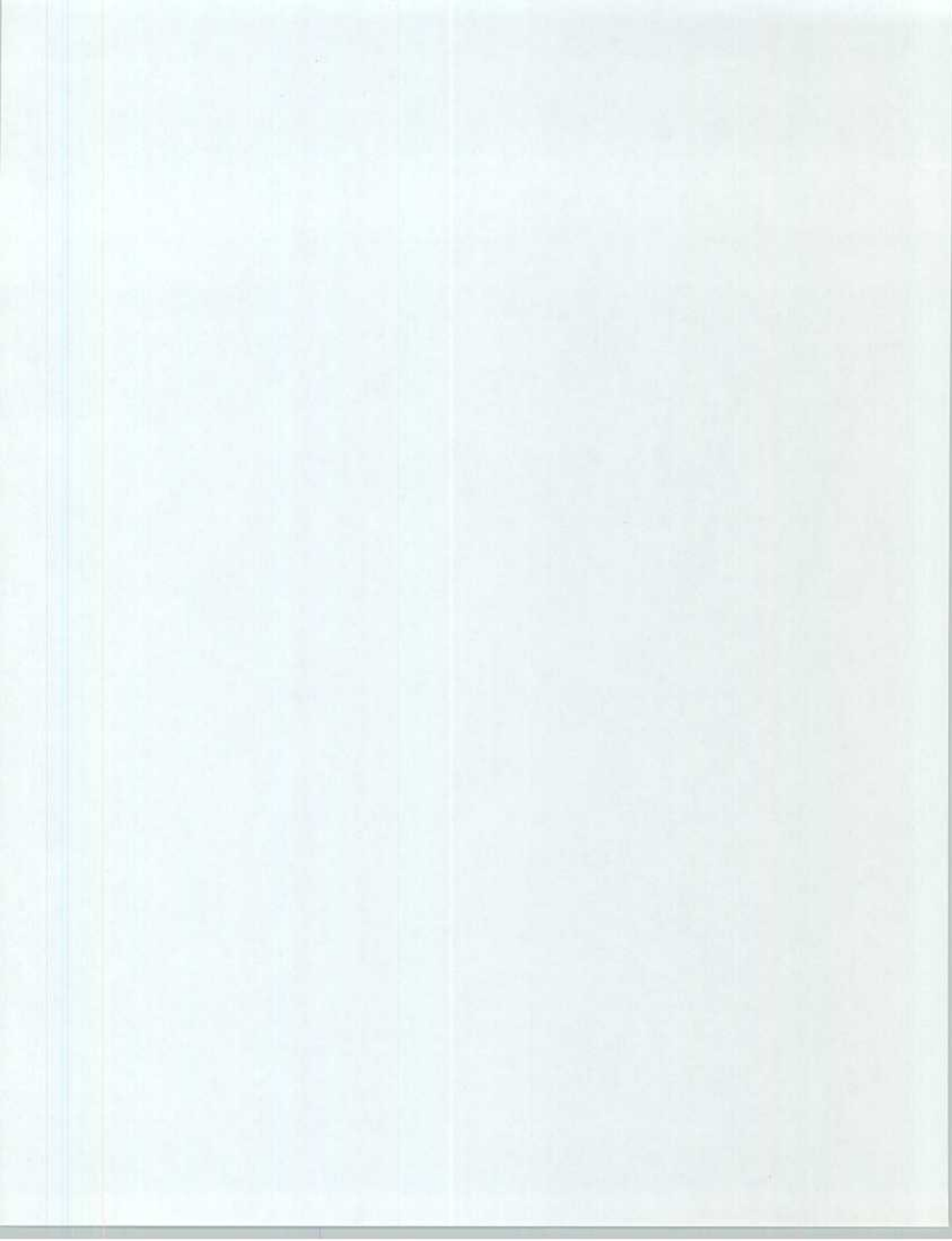
To: CG (First, Second, or Third) MarDiv

Classification (In accordance with content - CONFIDENTIAL or SECRET.)

Subj: MIJI Report (U)

1. Unit experiencing MIJI
2. Type Incident. Meaconing, intrusion, jamming, or interference.
3. Operator or POC, function, and AUTOVON number.
4. Weather conditions.
5. Nomenclature of equipment affected.
7. Date, time (Z), and coordinates MIJI began.
8. Date, time (Z), and coordinates MIJI most effective.
9. Date, time (Z), and coordinates MIJI ended.
11. Transmitter affected (callsign, frequency, type modulation, bandwidth).
12. MIJI (interfering signal) (callsign, frequency, bandwidth, type emission, or audio characteristic).
13. Use or purpose of frequency affected.
14. Other stations heard on frequency.
15. MIJI effectiveness (percent of copy lost).
16. Other stations or units confirming MIJI.
17. How did MIJI begin or end (faded, abruptly, victim or MIJI shifting frequency)?
18. ECCM used and results.
40. Narrative:
  - a. Summary - Operator explanation of just what happened.
  - b. List ships, ground units, or aircraft in vicinity that might be MIJI source.
  - c. State mission phase at time of incident (routine operations, in combat, flying to target, etc.).
  - d. Include the term "final report" if additional reporting is not anticipated.

MIJI Reports sent external to the Division by Division HQ shall be sent to units designated in the current edition of MCO 3430.3, info CG (I, II, or III) MAF.



## EW SOP

### APPENDIX D

#### STOP-BUZZER PROCEDURES AND FORMAT

1. GENERAL. The information contained in this appendix provides the necessary controls and command procedures to ensure safety and coordination of aggressor and friendly EW activities.

a. The codeword "STOP-BUZZER" will be passed via the STOP-BUZZER net, or the otherwise most expeditious means, including the net receiving the ECM.

b. Upon initiation of a "STOP-BUZZER", ECM operations will resume only upon clearance from higher headquarters and only when it has been determined the emergency condition no longer exists.

c. The unit imposing a "STOP-BUZZER" will submit a follow-up report to the CG MARDIV (ATTN: G-3/EWO) providing the following minimum information:

(1) Unit.

(2) Frequency.

(3) Location (Coordinates)

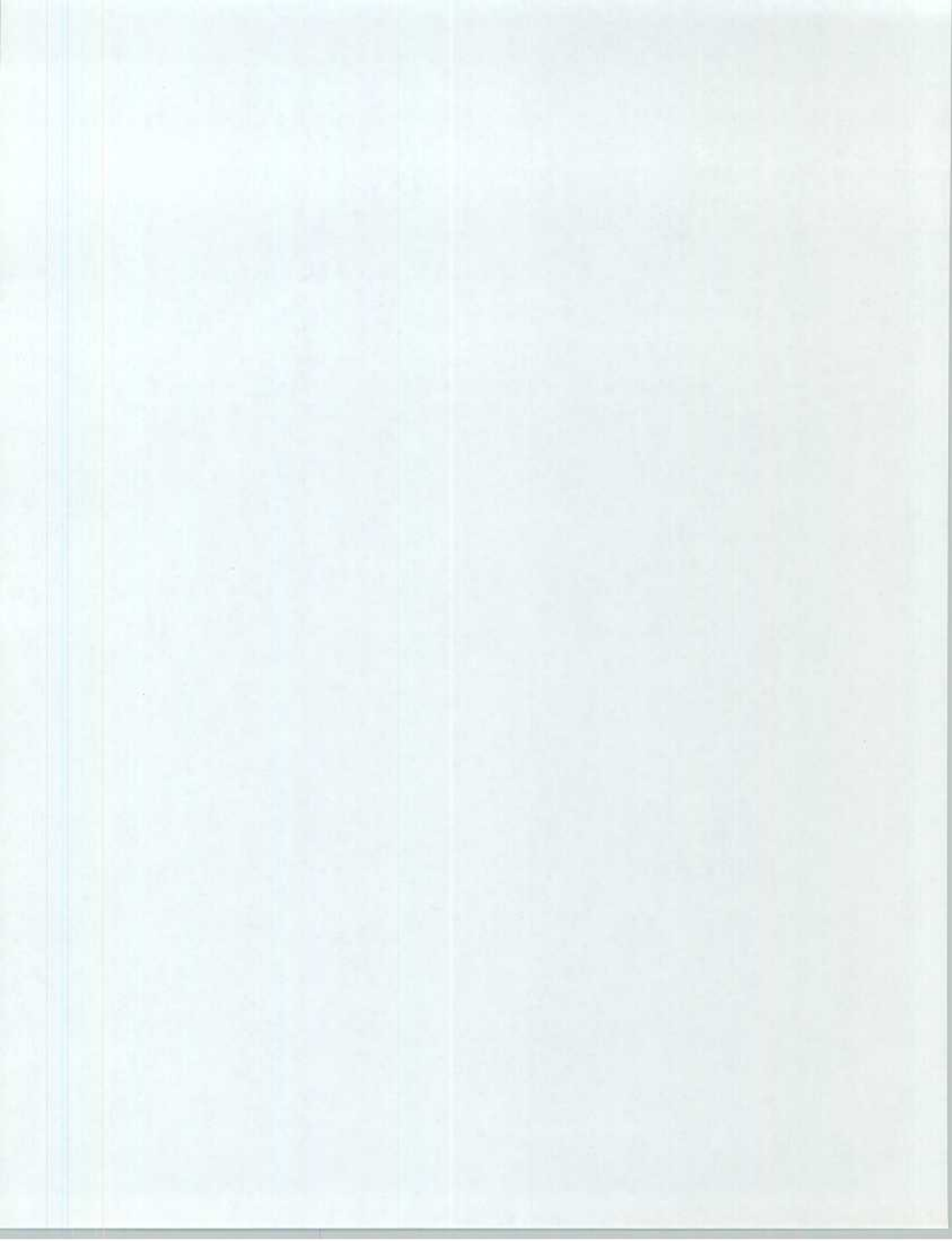
(4) Description of potential danger

(5) Estimated duration

(6) Minimum safeguards required to eliminate situations.

d. When the emergency situation has passed, a CLEAR-BUZZER message must be sent by the originator to indicate a safe condition.





EW SOP

APPENDIX E

FREQUENCY INTERFERENCE REPORT

1. The FIR, when formatted as directed below, is unclassified, and can be passed over any communication circuit or other communication means, i.e., telephone, runner, etc.

2. The FIR format is simple, as indicated below:

a. FROM: REPORTING UNIT

b. TO: NEXT HIGHER HQ (PASSING INSTRUCTIONS TO CEO/SYSCON  
AND EWO)

c. INFO: (SUPPORTING EW ASSET, IF AVAIL/APPROPRIATE)

d. UNCLAS

(1) FIR (TITLE, TO ALERT RECIPIENTS)

(2) FREQUENCY AFFECTED BY INTERFERENCE

(3) TIME OF INTERFERENCE

3. Time is critical. Report interference as soon as possible. Do not wait until it ends.



## EW SOP

### APPENDIX F

#### DIRECTIVES AND PUBLICATIONS

1. The current edition of the following directives/publications contain policies, guidance, instructions, and procedures pertaining to Electronic Warfare. Units are required to possess only those designated by an asterisk (\*); all other are "nice to have". (Read: overall classification, short title, classification):

##### MARINE CORPS

* MCO 3430.1	(U)	Performing ECM in the US and Canada (U)
* MCO 3430.2	(U)	Electronic Warfare (EW) Policy (U)
* MCO 3430.3	(U)	MIJI (U)
FMFM 2-3	(C)	Signal Intelligence/EW operations (U)
* MCDEC OH 3-4	(U)	EW Operations Handbook (U)
OH 10-2	(C)	Radio Bn Communications Requirements (U)

##### NAVY

OPNAVINST 3430.18	(U)	Reporting MIJI of Electromagnetic Systems (U)
NWP-33	(S)	Electronic Warfare (U)
NWP 12-6	(S)	Tactical EW Planning Guide (U)
CINCLANTFLTINST S3430.2	(S)	U.S. Atlantic Fleet EW Policy (U)
CINCLANTFLT/ CINCUSMAVEUR INST C3430.6	(C)	EW Equipment Configuration
NTP 4	(U)	Naval TELCOM Procedures Fleet Communications (C)
NWP 4	(U)	Basic Operational Communications (C)

##### ARMY

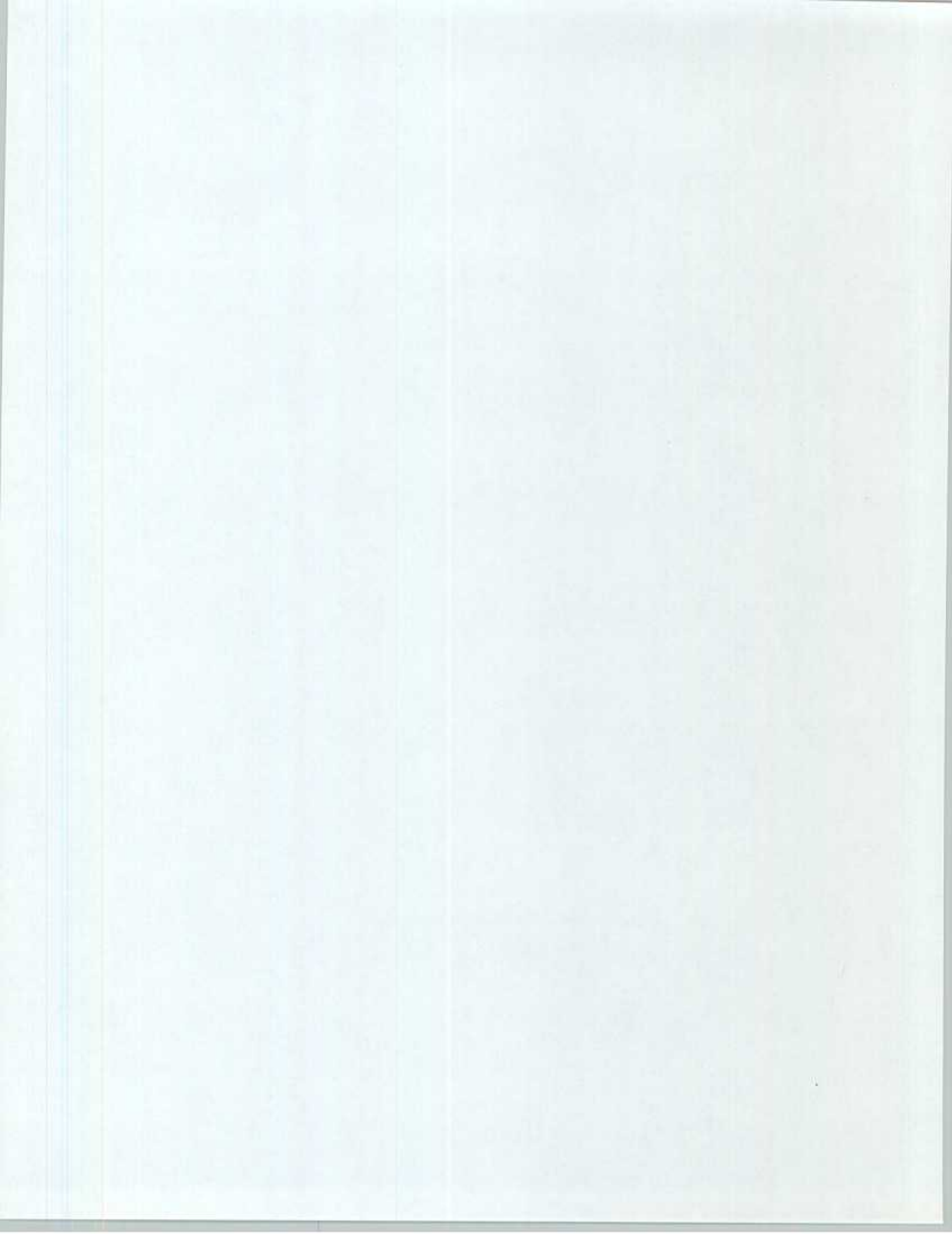
FM 32-20	(C)	Electronic Warfare (U)
FM 32-30	(C)	EW Tactics of Defense (U)
FM 100-5	(U)	Operations (Chapter 9 EW) (U)
TC 30-20	(U)	SIGINT (U)
TC 32-10	(U)	How to train EW (U)
TC 32-17	(C)	EW Operations (U)

##### AIR FORCE

AFR 51-3	(U)	EW Principals
AFR 55-90	(U)	EW Policy
AFM 100-43	(U)	C-E, EW

##### JCS

JCS PUB 23	(C)	Doctrine for SIGINT and ESM Support to Joint MIL OPS
------------	-----	--



## EW SOP

### APPENDIX G

#### EW REQUESTING PROCEDURES AND FORMAT (U)

REQUESTING PROCEDURES: EW support for tactical operations may be in two forms. The first method would be pre-planned ECM missions in support of planned operations. In this case, the request for ECM support should be submitted far enough in advance of the execution time to permit proper coordination. (Under normal conditions, these pre-planned ECM missions should be submitted no later than 12 hours prior to the operation). The second method would be in support of an "on going" operation where the commander determines the ECM support is vital to its successful completion. In the latter case, time would be the most critical factor and the request would be submitted by the most expeditious means utilizing the format outlined below.

CLASSIFICATION (Classified in accordance with current directives)  
PRECEDENCE (Immediate or Priority, depending on the urgency of request)

FROM: (Requesting Unit)

TO: CG MARDIV (ATTN: G-3/EWO)\*

1. REQUEST FOR EW SUPPORT

A. TYPE OF EW SUPPORT REQUESTED (jamming, intrusion, or location (DF)).

B. DATE/TIME TO START/STOP (all times local)

C. FREQUENCY (if known)

D. VICINITY OF COORDINATES ---- (6 digit)

E. TARGET (name of potential enemy)

\* - Appropriate Division 1st, 2d, and 3d.